# ROUTING AND RECORD SHEET

SUBJECT: (Optional)

Collateral Top Secret Control Program

| | | |
|---|---|---|
| FROM: [redacted]<br>Director of Information Services<br>1205 Ames | EXTENSION<br>[redacted] | NO.<br>OIS 85-258 STAT<br>DATE<br>14 June 1985 STAT |

| TO: (Officer designation, room number, and building) | DATE | | OFFICER'S INITIALS | COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.) |
|---|---|---|---|---|
| | RECEIVED | FORWARDED | | |
| 1. EO/DDA<br>7 D 18 Headquarters | 18 JUN 1985 | | | Maybe we need "Tiger Teams" similar to the ones who did the wholesale screening STAT [redacted] for weeks at a time. Every Directorate & component put up manpower to do it and it worked fine. |
| 2. | | | | |
| 3. ADDA | | | | |
| 4. | | | | |
| 5. DDA | 18 JUN 1985 | | | |
| 6. | | | | |
| 7. | | | | |
| 8. DDA Reg (file) | | | | DD/A REGISTRY<br>FILE: 70-1 |
| 9. | | | | |
| 10. | | | | |
| 11. | | | | |
| 12. | | | | |
| 13. | | | | |
| 14. | | | | |
| 15. | | | | |

85-2169

OIS 85-258

14 June 1985

MEMORANDUM FOR: Deputy Director for Administration

FROM: [redacted] 25X1
Director of Information Services

SUBJECT: Collateral Top Secret Control Program

Harry:

1. In February 1984 I shared with you my concerns over deficiencies in the Top Secret control program. Two of these deficiencies--automated tracking system and organization placement of the program--were handled within OIS resources. You provided needed funding for the hiring of Independent Contractors so as to tackle the third deficiency--number of personnel dedicated to the program. Our latest status report is attached; it shows that we are making progress but the progress is slow.

2. My concern over security, the security of information that, by definition, could cause exceptionally grave damage to the national security, has been heightened by the Walker spy case. If due to this case there is a review of how classified information is handled within the Government and it becomes known that thousands of unaccounted for documents are "floating" within CIA, there could be a great deal of embarrassment and maybe even some strong criticism. When I first brought this to your attention, I feared a scandal if the situation ever leaked to the press. Imagine what the reaction would be today in the "Walker" climate.

3. You may wish to further preclude any potential embarrassment or criticism to the Agency by including in the supplemental Security monies you have requested resulting from the Walker case, additional funding for annuitants to locate~~d~~ unaccountable Top secret ~~Document~~ documents. This is a labor-intense effort and the best way to clean this act up quickly is to put more people on it. Unfortunately, people continue to cost money.

[redacted] 25X1

Reclassify ADMINISTRATIVE
INTERNAL USE ONLY when
attachment removed

4. Harry, I have also a paper done three years ago on document security that you may want to read. I believe it is still relevant as it discusses how much control and inconveniences will be tolerated in the flow of information around the Agency. We opted in favor of ease of access rather than tight controls. We may need to revisit this decision.

[redacted]

25X1

Attachments

## Unaccounted for Top Secret Collateral Documents
## by
## Agency Directorate

| | December 1983 | December 1984 | January 1985 | June 1985 |
|---|---|---|---|---|
| DDI | 5,694 | 4,881 | 4,813 | 4,685 |
| DDS&T | 3,372 | 3,096 | 3,086 | 3,053 |
| DDO | 1,712 | 1,586 | 1,581 | 1,554 |
| DCI | 1,538 | 1,129 | 1,123 | 1,102 |
| DDA | 238 | 123 | 137 | ~~127~~ 64 |
| Total | 12,554 | 10,815 | 10,740 | 10,521 |

[redacted] 25X1

## Document Security

The present system of protecting documents by means of classification markings and access controls can be effective. It makes efficient use of security resources by protecting each document according to the sensitivity of the information it contains.

In practice, however, the effectiveness of the system varies because document security requirements tend to conflict with other demands. These demands can be grouped in three areas: volume, the need to use information, and the cultural environment. A fourth area, technology, permeates the other three in terms of both problems and solutions.

In recent years, as a result of technological advances in collection systems, telecommunications systems, computers, word processors, and copiers, the volume of national security information has been growing exponentially. Leading this growth has been the sensitive compartmented information (SCI) associated with special access programs. The increase in SCI documents has outstripped the resources devoted to controlling them, with a result that less-sensitive but lower-volume collateral information often is controlled more closely than SCI. For example, control of all non-electrical Agency collateral Top Secret documents has been partially automated in the TSCADS system for several years.

Although there are some automated SCI document control systems, as well as some automated registries that control all documents they receive, there has been no general application of technology to facilitate control of the large volume of documents we handle today. There is some ongoing research into control techniques such as optical bar coding and non-reproducible documents, and there is an Agency development program named TRIS to automate our records accounting systems, but further investment in technological solutions to document control problems is necessary if we are to protect our current volume of classified documents effectively.

In the area of information use, there is a basic conflict between document control and timely dissemination. Analysts and intelligence customers need information as quickly as possible, but control systems usually involve at least some delay. This conflict is compounded by the availability of office copiers and the ability of computer systems to provide "soft" as well as "hard" copies of documents almost instantaneously to many users. Although technology can help in this area, the balance between control and access must be drawn by management decision. For example, the fact that the TSCADS system does not include electrically transmitted documents reflects a management decision that speed is more important than Top Secret document control. Improving document security in this area requires a shift in management emphasis.

The area of cultural environment involves the manner in which the access to classified documents and the handling of them are controlled. In theory, effective document security requires hiring only trustworthy people, giving them access only to information they need to know, monitoring their compliance with document control requirements, and imposing stringent penalties for procedural violations. The problem in this area is that people these days do not want to put up with such controls. An example of the conflict in this area is the building entrance checks instituted by the Agency after the Kampiles incident. The scope of these checks had to be reduced due in part to the perceived inequity of inspecting women's handbags but not men's pockets. In an "ideal" document control system both would be inspected, but this is just not acceptable to today's employee.

Document control necessarily involves some inconveniences to, or impositions on, the people who use classified information. Although there is little, if anything, we can do about the cultural attitudes of our society, management could place more emphasis on the need for employees at all grade levels to put up with a certain amount of inconvenience in the interest of protecting classified documents.

Beyond the specific areas mentioned above, there are more general problems in the government's document security programs. Foremost among these is the multiplicity of inconsistent document control procedures we have to deal with. The ill-fated APEX exercise was in part an attempt to employ document security resources more effectively by concentrating them on truly sensitive information, using common document control procedures. Although the APEX approach failed, there is still much that can be done to establish consistent procedures. Once again, management emphasis is required to overcome competing interests among agencies.

There is also an overall question as to whether the classification system is an adequate basis for protecting sensitive information, particularly technological information. In answer to that question, Executive Order 12356 should enable us to classify any information that warrants protection. Cases such as Kampiles and Boyce/Lee, however, have demonstrated the obvious fact that classification alone is not sufficient. Effective document security requires a policy decision that we are willing to pay the costs of controlling documents after they are classified.